IN THE CLAIMS

1-9. (Cancelled)

10. (Currently Amended) An information security apparatus that ensures secure handling of predetermined information by computing an elliptic curve exponentiation of $k*Q$, based on computational complexity of solving a discrete logarithm problem on an elliptic curve $E:y^2=x^3 +$ ~~$a X x+ b$~~ $a \times x+b$ defined over a residue field F with a prime p being a modulus, comprising:

an information obtaining unit operable to obtain a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a first storage unit operable to store therein a coefficient a that is a linear term of the elliptic curve E;

a computation unit operable to compute an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment unit operable to judge whether the point Q and the obtained exponentiation-result-point $k*Q$ are on the elliptic curve E; and

a prohibition unit operable to prohibit an output of the obtained exponentiation-result-point $k*Q$, when a judgment result of the judging unit is negative; and

a processing unit operable to realize, when the judgment result of a judging unit is affirmative, ~~process~~ one of the processes of: encryption of a plaintext, decryption of a ciphertext; generation of a signature for a plaintext; signature verification for a plaintext and a

signature; or a process of sharing of a secret key between two parties without revealing the secret key to a third party, with the use of the obtained exponentiation-result-point $k*Q$; [[and]]

wherein the information obtaining unit obtains coordinates (Qx, Qy) as the point Q,

the computation unit computes coordinates (Qx', Qy') as the exponentiation-result-point $k*Q$, and

the judgment unit judges whether the point Q and the exponentiation-result-point $k*Q$ are on the same elliptic curve, by judging whether $(Qy^2-Qx^3-aXQx) - (Qy'^2- Qx'^3-aXQx') = 0$; and

an output unit configured to output one of an encrypted text, a decrypted ciphertext, signature data, a verification result, and a shared key.

11-14. (Cancelled)

15. (Currently Amended) An information security method for use in an information security apparatus that ensures secure handling of predetermined information by computing an elliptic curve exponentiation of k*Q, based on computational complexity of solving a discrete logarithm problem on an elliptic curve E: $y^2=x^3+a\times x+b$ defined over a residue field F with a prime p being a modulus, and that includes an information obtaining unit, a first storage unit storing a coefficient a that is a linear term of the elliptic curve E, a computation unit, a judgment unit, a prohibition unit, and a processing unit, the method comprising:

executing an information obtaining step by the information obtaining unit for obtaining a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

executing a computation step by the computation unit for computing an elliptic curve exponentiation of the exponent k and the point Q using the coefficient *a* stored in the first storage unit, to obtain an exponentiation-result-point k*Q;

executing a judgment step by a judgment unit for judging whether the point Q and the obtained exponentiation-result-paint k*Q are on the elliptic curve E;

executing a prohibition step by the prohibition unit for prohibiting an output of the obtained exponentiation-result-point k*Q, when a judgment result of the judgment step is negative; [[and]]

executing a processing step by the processing unit for realizing, when the judgment result of the judgment step is affirmative, one of the processes of: encryption of a plaintext, decryption of a ciphertext; generation of a signature for a plaintext; signature verification for a plaintext and a signature; or a process of sharing of a secret key between two parties without revealing the secret key to a third party, using the obtained exponentiation-result-point k*Q,

wherein, in the information obtaining step, the information obtaining unit obtains coordinates (Qx, Qy) as the point Q;

in the computation step, the computation unit computes coordinates (Qx', Qy') as the exponentiation-result-point k*Q; and

in the judgment step, the judgment unit judges whether the point Q and the exponentiation-result-point k*Q are on the same elliptic curve, by judging whether $(Qy^2 - Qx^3 - a \times Qx) - (Qy'^2 - Qx'^3 - a \times Qx') = 0$; and

an output unit configured to output one of an encrypted text, a decrypted ciphertext, signature data, a verification result, and a shared key.

16. (Currently Amended) A computer program stored on a computer readable medium which, when executed on a computer, performs each of the steps of the method of Claim 15.

17. (Currently Amended) The computer program stored on a computer readable medium of Claim 16, recorded on a computer-readable recording medium.